Claims

1. A method for real-time betting, within a communications system comprising a distributed domain and central domain, by handling electronic records that contain predictions of the outcome of a certain incident, comprising the steps of:

- generating, within the distributed domain, a multitude of electronic records that contain predictions of the outcome of the incident, according to players' inputs,
- furnishing, within the distributed domain, each of the electronic records with a cryptographically protected proof of a certain moment of a distributed domain time associated with the generation of the electronic record,

characterized in that the method further comprises the steps of:

- receiving, within the distributed domain, repetitive beacon tick packets and watchdog tick packets, comprising time information of local time of the central domain at the moment the packet was sent,
- synchronising local time of the distributed domain, with time equated with the central domain time information received by the beacon tick packets, by help of values of a counter in the distributed domain and time information in received beacon tick packets, and
- verifying validity of local time of the distributed domain regarding to the central domain's local time by comparing local time of the distributed domain to time information relating to local time of the central domain received by the watchdog tick packets.

2. A method according to claim **1, characterized** in that the synchronisation of local time of the distributed domain comprises the steps of:

- receiving, within the distributed domain, repetitive first and second beacon tick packets broadcasted by a predetermined time interval and reading a value of the counter at the moment of receiving the first and second beacon tick packets, in order to create a conversion factor comparable to the interval of the first and second received beacon tick packets and to the values of the counter at the moments of receiving the first and second beacon tick packets,
- sending a request from the distributed domain to the central domain to send a response to indicate accurate central domain's local time at the moment of receiving the request (t_1) and at the moment of sending the response (t_2),
- initialising a clock indicating local time of the distributed domain (t_0),

- receiving the response from the central domain and reading time information of the central domain's local time (t_1 and t_2) and a value of the counter at a moment of receiving the response, in order to construct a clock offset by computing an average delay between t_1, t_0 and t_3, t_2, and
- updating new local time of the distributed domain essentially equating to the central domain's local time by adding to latest local time (t_0) of the distributed domain the clock offset and a value derived by multiplying with the conversion factor the difference of the values of the counter at the moment of receiving the response from the central domain and at the moment of sending the request to the central domain.

3. A method according to claim 1, **characterized** in that the betting process is an off-line betting process.

4. A method according to claim 1, **characterized** in that the beacon tick packets and watchdog tick packets are broadcasted by a predetermined time interval.

5. A method according to any of preceding claims, **characterized** in that the beacon tick packet, being protected information packet broadcasted to a distribution domain regularly, comprises at least one of the following information: time information relating to central domain's local time at a moment the beacon tick packet was sent from the central domain, delay of the next coming beacon tick packet to be broadcasted to the distributed domain, security parameters, and message authentication code.

6. A method according to claim 1, **characterized** in that the watchdog tick packet comprises at least one of the following information: time information relating to central domain's local time at a moment the watchdog tick packet was sent from the central domain, delay of the next coming watchdog tick packet to be broadcasted to the distributed domain, security parameters, key updates and message authentication code.

7. A method according to claim 1, **characterized** in that delay of the next coming watchdog and/or beacon tick packet is compared to delay information announced in the previous watchdog and/or beacon tick packet, and the watchdog and/or beacon tick packet is accepted only if the delay of the next coming watchdog and/or beacon tick packet is valid.

8. A method according to claim 1, **characterized** in that the beacon tick packets and watchdog tick packets are broadcasted from the central domain.

9. A method according to claim 1, **characterized** in that the beacon tick packets are broadcasted by a Digital Audio Broadcasting transmitter arrangement and/or a Digital Video Broadcasting transmitter arrangement.

10. A method according to claim 1, **characterized** in that an interval from the player's input to latest and/or to next beacon tick packet is measured either in terms of counter values or of distributed domain's local time, and stored in a cryptographically form with the player's input to the electronic record.

11. A method according to claim 1, **characterized** in that a value of the counter and/or an electric clock signal representing the local time of the distributed domain at the said moment is used as an input in generating a cryptographically protected proof of a certain moment of a distributed domain.

12. A method according to claim 1, **characterized** in that the counter is a free running independent counter, and the distributed domain comprises more than one counter the rate of which are constant and independent of each other, and in that values of the first counter are used for internal log of events and returned to the central domain, and values of the second counter are used for time service of the distributed domain.

13. A method according to claim 1, **characterized** in that stored data, a value of the counter and/or an electric clock signal representing the local time of the distributed domain are chained by help of a key.

14. A computer program product directly loadable into the internal memory of a digital computer, **characterised** in that it comprises software code portions for performing the steps of claim 1 when said product is run on a computer.

15. A computer program product stored on a computer usable medium, **characterised** in that it comprises computer readable program means for causing a computer to perform the steps of claim 1 when said product is run on a computer.

16. A terminal for real-time betting, within a communications system comprising a distributed domain and a central domain, where the terminal belongs to the distributed domain, by handling electronic records that contain predictions of the outcome of a certain incident, is arranged to:

- generate, within the distributed domain, an electronic record that contains a prediction of the outcome of the incident, according to a player's input,

- furnish, within the distributed domain, the electronic record with a cryptographically protected proof of a certain moment of a distributed domain time associated with the generation of the electronic record,

characterized in that the terminal is further arranged to:

- receive, within the distributed domain, repetitive beacon tick packets and watchdog tick packets, comprising time information of local time of the central domain at the moment the packet was sent,
- synchronise local time of the distributed domain, with time equated with the central domain time information received by the beacon tick packets, by help of values of a counter in the terminal and time information in received beacon tick packets, and
- verify validity of local time of the distributed domain regarding to the central domain's local time by comparing local time of the distributed domain to time information relating to the local time of the central domain received by the watchdog tick packets.

17. A terminal according to claim 16, **characterized** in that the terminal is, when synchronising of local time of the distributed domain, arranged to:

- receive, within the distributed domain, repetitive first and second beacon tick packets broadcasted by a predetermined time interval and read a value of the counter at the moment of receiving the first and second beacon tick packets, in order to create a conversion factor comparable to the interval of the first and second received beacon tick packets and to the values of the counter at the moments of receiving the first and second beacon tick packets,
- send a request from the distributed domain to the central domain to send a response to indicate accurate central domain's local time at the moment of receiving the request (t_1) and at the moment of sending the response (t_2),
- initialise a clock indicating local time of the distributed domain (t_0),
- receive the response from the central domain and read time information of the central domain's local time (t_1 and t_2) and a value of the counter at a moment of receiving the response, in order to construct a clock offset by computing an average delay between t_1, t_0 and t_3, t_2, and
- update a new local time of the distributed domain essentially equating to the central domain's local time by adding to latest local time (t_0) of the distributed domain the clock offset and a value derived by multiplying with the conversion factor the difference of the values of the counter at the moment of receiving the response from the central domain and at the moment of sending the request to the central domain.

18. A terminal according to claim 16, **characterized** in that the terminal is and off-line terminal.

19. A terminal according to claim 16, **characterized** in that the terminal is arranged to compare delay of the next coming watchdog and/or beacon tick packet to delay information announced in the previous watchdog and/or beacon tick packet, and accept only the watchdog and/or beacon tick packet if delay of the next coming watchdog and/or beacon tick packet is valid.

20. A terminal according to claim 16, **characterized** in that terminal is arranged to measure an interval from the player's input to latest and/or to next beacon tick packet either in terms of counter values or of distributed domain's local time, and store it in a cryptographically form with the player's input to the electronic record.

21. A terminal according to claim 16, **characterized** in that terminal is arranged to use a value of the counter and/or an electric clock signal representing local time of the distributed domain at the said moment as an input in generating a cryptographically protected proof of a certain moment of a distributed domain.

22. A terminal according to claim 16, **characterized** in that the counter is a free running independent counter, and the terminal comprises more than one independent counter the rate of which are constant and independent of each other, and in that values of the first counter are used for internal log of events and returned to the central domain, and values of the second counter are used for time service of the distributed domain.

23. A terminal according to claim 16, **characterized** in that the terminal is arranged to read a value of the free running counter and store it in a memory means of the terminal for later user or verification, when at least one of the following event occurs: an information packet is received within the terminal, and the player makes an action, such as places his/her bet.

24. A terminal according to claim 16, **characterized** in that the terminal comprises a watchdog for performing functional steps of any method claims 1-13.

25. A terminal according to claim 24, **characterized** in that the watchdog is arranged to inform the central domain of values of the counter by sending information of counter values to the central domain.

26. A terminal according to claim 24, **characterized** in that the watchdog is performed within a protected integrated circuit.

27. A terminal according to claim 16, **characterized** in that the terminal comprises a data network access means (1206) for establishing two-way data link between the terminal and the central domain for bet record storage initialisation and transferring broadcast parameters.

28. A terminal according to claim 16, **characterized** in that the terminal comprises a broadcast reception means (1208) for establishing one-way data link between the terminal and the central domain for transferring beacon tick packets and watchdog tick packets, watchdog key update packets, and bet start/end packets from central domain to the terminal (1200).

29. A terminal according to claim 24, **characterized** in that the watchdog (1210) comprises also timing means (1214) being responsible for controlling that watchdog tick packets are received and that they are received at right time, and for adjusting local time of the terminal according to received data packets.

30. A terminal according to claim 24, **characterized** in that the watchdog (1210) comprises a communication protection means (1216) for encrypting and decrypting communication and checking signatures, storage key management means (1218) for creating and updating keys for storing data, such as placed bets, and storage entry generation means (1220) for encrypting and chaining entries, adding time-stamps and/or counter values to data, such as placed bets, and watchdog software means (1222), which are responsible for authentication of a player, and processing of application data.

31. An organiser server for real-time betting, within a communications system comprising a distributed domain and a central domain, where the organiser server belongs to the central domain, by handling electronic records that contain predictions of the outcome of a certain incident, is arranged to:

- receive from the distributed domain a multitude of electronic records that contain predictions of the outcome of the incident and,
- process for finding out, after the outcome of the incident is known, which of the electronic records, if any, contain correct predictions of the outcome of the incident,

characterized in that the organiser server is further arranged to:

- send repetitive beacon tick packets and watchdog tick packets, comprising time information of local time of the central domain at the moment the packet was sent, to the distributed domain, in order that local time of the distributed domain is synchronised with time equated with the central domain time information received by the beacon tick packets, by help of values of a counter in the distributed domain and time information in received beacon tick packets, and verify validity of local time of the distributed domain regarding to the central domain's local time by comparing local time of the distributed domain to time information relating to the local time of the central domain received by the watchdog tick packets.

32. An organiser server according to claim 31, **characterized** in that the organiser server, when synchronising of local time of the distributed domain, is arranged to:
- send repetitive first and second beacon tick packets in predetermined time interval to the distributed domain, in order to create, within the distributed domain, a conversion factor comparable to the interval of the first and second received beacon tick packets and to the values of the counter at the moments of receiving the first and second beacon tick packets within the distributed domain, and
- respond to a request of the distributed domain to send a response to indicate accurate central domain's local time at the moment of receiving the request (t_1) and at the moment of sending the response (t_2).

33. An organiser server according to claim 31, **characterized** in that the organiser server is arranged to wait a predetermined time interval announced in the previous beacon/watchdog tick packet, until send the next beacon/watchdog tick packet.

34. An arrangement for real-time betting, comprising a distributed domain and a central domain, by handling electronic records that contain predictions of the outcome of a certain incident, is arranged to:
- generate, within the distributed domain, a multitude of electronic records that contain predictions of the outcome of the incident, according to a players' inputs,
- furnish, within the distributed domain, each of the electronic records with a cryptographically protected proof of a certain moment of a distributed domain time associated with the generation of the electronic record,

characterized in that the arrangement is further arranged to:

- receive, within the distributed domain, repetitive beacon tick packets and watchdog tick packets, comprising time information of local time of the central domain at the moment the packet was sent,
- synchronise local time of the distributed domain, with time equated with the central domain time information received by the beacon tick packets, by help of values of a counter in the distributed domain and time information in received beacon tick packets, and
- verify validity of local time of the distributed domain regarding to the central domain's local time by comparing local time of the distributed domain to time information relating to the local time of the central domain received by the watchdog tick packets.

35. An arrangement according to claim 34, **characterized** in that an information traffic between the central domain and distributed domain is encrypted.

36. An arrangement according to claim 34, **characterized** in that the arrangement comprises a two-way data link used for collecting bet records from the bet record storage within the distributed domain to the central domain.

37. An arrangement according to claim 34, **characterized** in that the arrangement comprises an one-way data link for transferring beacon tick packets and watchdog tick packets, watchdog key update packets, and bet start/end packets and results from central domain to the terminal within the distributed domain.

38. A circuit means for real-time betting, within a communications system comprising a distributed domain and a central domain, where the circuit means belongs to the distributed domain, by handling electronic records that contain predictions of the outcome of a certain incident, is arranged to:

- generate, within the distributed domain, an electronic record that contains a prediction of the outcome of the incident, according to a player's input,
- furnish, within the distributed domain, the electronic record with a cryptographically protected proof of a certain moment of a distributed domain time associated with the generation of the electronic record,

characterized in that the circuit means is further arranged to:

- receive, within the distributed domain, repetitive beacon tick packets and watchdog tick packets, comprising time information of local time of the central domain at the moment the packet was sent,
- synchronise local time of the distributed domain, with time equated with the central domain time information received by the beacon tick packets, by help

of values of a counter in the terminal and time information in received beacon tick packets, and

- verify validity of local time of the distributed domain regarding to the central domain's local time by comparing local time of the distributed domain to time information relating to the local time of the central domain received by the watchdog tick packets.